



Friday, August 26, 2024

Erik Beith
Competition Policy Division
Federal Communications Commission
45 L Street Northeast
Washington, District of Columbia 20554

Aloha mai kāua e Mr. Beith,

I am writing to share our Robocall Mitigation Program with the Federal Communications Commission and to confirm and certify that all voice traffic that originates from or on the mobi network is STIR/SHAKEN authenticated, in compliance with regulations established by the FCC under 47 CFR § 64.6301(a) in furtherance of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act.

As a carrier member of the CCA (the Competitive Carriers Association) and the CTIA (formerly the Cellular Telecommunications and Internet Association), as an operator member of the GSMA, and as a member of MEF (the Mobile Ecosystem Forum) and the Pacific Telecommunications Council (commonly, PTC), we strongly support the efforts the Commission has taken to stop our shared networks from being used to carry fraudulent and illegal calls, both through more broadly and, particularly, through the implementation of STIR/SHAKEN.

As detailed below, and as required by the Commission, we and our partners have put in place commercial, operational, and technological systems, processes, and safeguards to ensure that we do not originate, carry, nor process illegal robocall traffic on our network, pursuant to 47 C.F.R. § 64.6305(a).

We believe that it may help to have a brief background of our current network model and

mobi is built with aloha from Hawai'i, by team members from many places and many walks of life.

mobi, Inc.

We acknowledge that Her Majesty, Queen Lili'uokalani, as the Sovereign Monarch of the Kingdom of Hawai'i, yielded only under duress to avoid bloodshed, and that Her people remain unjustly deprived of their rights to self-determination. Our Kama'āina respect and recognize many generations of Kanaka, their aloha, their sacrifice, and their knowledge systems have shaped and continue to shape Hawai'i. For this, a no ko mākou mahalo like 'ana a me ke aloha, we are infinitely grateful. We stand in solidarity with our communities throughout Hawai'i, and we seek to support, both as a company and as a team, the strategies and work of Native Hawaiians to protect their communities and this 'āina, their 'āina.

1668 S. King St., Ste. 101
Honolulu, Hawai'i 96826

+1 808 723-1111

mobi.com

how that impacts our STIR/SHAKEN implementation, to better understand the steps we have taken in context and why they necessarily go beyond the steps a typical wireless carrier or voice services provider may have chosen to deploy, particularly in context of our mobile app-first digital and eSIM onboarding path for customers outside of our native footprint in Hawai'i.

Our hybrid MNO + MVNO model, with our 5G core

mobi launched in 2005 as the only facilities-based regional wireless carrier serving Hawai'i. Today, we operate as a hybrid mobile network operator (MNO) within portions of our own footprint, and as a mobile virtual network operator (MVNO) elsewhere domestically.

Following a transaction in 2015 in which the majority of our spectrum and radio access network (RAN) were acquired by an entity of Verizon Wireless, most of our wireless subscribers were eventually migrated to be served from their mobile core. Last year, we announced that we would shift from our own legacy core to a modern, cloud-based core built and operated by Working Group Two, a startup created by Telenor and since acquired by Cisco, which offers considerably greater scalability, redundancy, and technological capabilities (including in the area of detecting and mitigating robocalls and other abusive and illegal activities).

As a result of the 2015 transaction, many of our subscribers are served today through a "thin" or "light" MVNO model, although we are migrating those customers to a "thick" or "full" MVNO model, whereby a customer will be served from our own mobile core network (regardless of whether they are "roaming" often or even permanently on the RAN of a partner mobile network).

Our Know Your Customer procedures

mobi takes significant steps to prevent bad actors from originating illegal calls from our network, including through a number of Know Your Customer procedures, which are in addition to our fraud prevention program. The latter is intended to both validate and, where necessary, augment data that we receive through existing KYC processes both proactively and, when and where necessary, reactively, based on certain flags, industry data sets, specific usage patterns, or other automated and manual triggers and signals. Our fraud prevention program also helps us evolve our KYC processes over time, by highlighting areas where additional data or data sources, directly or indirectly, could be helpful in improving our visibility into, particularly, the authenticity of any given new customer account.

In our terms and conditions, we make clear that a subscriber account is for personal use and cannot be used for commercial purposes, including “telemarketing, commercial research, or commercial data collection; any fraudulent, obscene, illegal, harassing or abusive purpose,” nor for “unsolicited voice, text, e-mail, or other transmittals,” nor anything that “could be considered unsolicited commercial communication.” We make it clear that we consider it “abuse to use [our network] in violation of any laws or regulations,” and that we will take action “to protect you, other mobi users, mobi, and other carriers [and their customers] from fraud, abuse, or unlawful use of [our network].”

Although we do have and, of course, allow business customers and accounts, the subscriptions (or SIMs/eSIMs) on such accounts are expected and only permitted to be used by a distinct individual for their own use, including in furtherance of their profession to the extent it does not otherwise violate our terms of service. While we do regularly receive inquiries about utilizing our services for primarily or entirely outbound voice or messaging traffic, we do not offer such services and do not intend to do so, and direct these inquiries to providers that specialize in delivering such capabilities. To the very limited extent a prospective or new “customer” has attempted to or successfully activated service with us for such purposes, we have blocked the activation of service if we suspect, or terminated their services if already active upon detection of, such usage (and without regard to any stated good faith on their part, as our services are expressly not intended for nor permitted to be utilized for such traffic).

Regardless of the stated purpose (if any) of a given customer or account, prospective or existing, we have policies and procedures in place to detect, prevent, and prohibit bad actors from impersonating others, from using fake or forged headers, from fabricating domain names, emails, and telephone numbers, in addition to other types of deceptive addressing and spoofing that can be used to secure access to telecommunication networks for illegal purposes. We reserve the right to not activate, to suspend, or to terminate an account, without notice if necessary, for engaging in any of those prohibited practices, and we have the ability to block voice and other traffic when and where necessary.

As mentioned further below, we apply these terms, policies, and processes to all subscribers, regardless of whether they are served from our own core or through a partner network.

Our Know Your Upstream Provider procedures

mobi has partnered with Sinch to provide infrastructure and services necessary for inbound and outbound voice and messaging capabilities and interconnection for subscribers served from our own core. When not accessing the mobi network directly, these customers are or will be served through various roaming and other wholesale access agreements with partners or providers, such as T-Mobile (and, previously, Sprint), Carolina West Wireless, Inland Cellular, and UScellular domestically, and Bell Canada, Claro, Eircom, Liberty, Salt, Telus, and Vodafone internationally, directly or via our intercarrier roaming partnerships with BICS, Comfone, and TNS (Transaction Network Services).

In addition to our subscribers that will be served via Sinch and its subsidiaries and affiliates, for our subscribers that are hosted within the Verizon Wireless core network, we both inherit comparable systems and capabilities, and are mutually contractually-obligated to prevent, mitigate, and act upon abuse, spam, fraud, and other illegal activities that are flowing from, to, or through our networks. Although we may have different visibility into their systems and processes vis-à-vis Sinch, we have found both to be, and expect both to continue to be equally vigilant in preventing illegal calls from reaching our customers and in assisting us in identifying, investigating, and stopping any calls that may pass through or originate from within our network.

Our partnership with Sinch includes services delivered via its Sinch Voice units (particularly, Inteliquent, Onvoy, and Neutral Tandem), which have each certified their complete STIR/SHAKEN implementations in the Robocall Mitigation Database, and filed their Robocall Mitigation Programs as gateway providers, most recently updated in their filing on February 26, 2024. Separately, we effectively inherit the same program and processes implemented by Verizon Wireless (under its Cellco Partnership entity), as filed on February 23, 2024.

Contractually, mobi and our partners must and do work together to meet any and all regulatory obligations, and to provide information required by the FCC and by other state or local regulatory authorities, and to investigate and action any suspected or actual external reports or internal alerts relating to fraud, spam, or other abuse, including robocalls. Both mobi and, as shared in their own program descriptions, Sinch and Verizon have automated processes in place to identify and stop unusual traffic pending further investigation, and we both have active, around-the-clock fraud monitoring and detection and mitigation processes and capabilities for both national and international calls.

As a policy and practice, both mobi and our carrier partners work to address unlawful use in a timely manner and will work cooperatively with industry peers and colleagues, law enforcement agencies, governmental entities, regulatory authorities, and other carriers, to address issues and reports related to illegality, fraud, and abuse. mobi does and will continue to use commercially reasonable efforts to prevent unauthorized, illegal, and fraudulent use of the services that are provided to use by or via our upstream carriers, and we do and shall terminate any unauthorized, illegal, or fraudulent user access. mobi, as well as Sinch and Verizon, do and must cooperate fully with traceback requests, and both of our companies do and will continue to take commercially-reasonable action on offending numbers in order to minimize misuse.

Sinch requires all connecting carriers, including mobi, to provide STIR/SHAKEN for our own outbound calls in a manner that is consistent with Commission requirements, and requires the same now for inbound calls to our own subscribers from other carriers. While Verizon does not operate strictly as a gateway provider, they do implement similar requirements for the other carriers they interconnect with or accept traffic from, and have committed to continuing to do so as a matter of course.

Based on the signalling provided via STIR/SHAKEN, and as augmented through data sources available to us from Sinch, netnumber, NeuStar, TNS, and other partners, we also have the ability to “tag” incoming calls with reputation scoring, to help protect our customers from unwanted robocalls and other unsolicited calls. As a result, calls with a reputation score that falls below a given threshold can be tagged with an indicator that an iPhone or Android device can then use to alert our customer (for example, as “potential spam” or “scam likely”). This indicator can then help our customer determine whether to answer the call (and, if so, to treat any information provided or action requested with greater scrutiny than might otherwise have been the case). To further these capabilities, our carrier partners tag or carry tags for calls identified as spam or fraudulent to us when passing these calls to us via our interconnections with their networks.

In addition to signalling provided or passed to us by Sinch and other network partners, mobi also uses our own fraud management capabilities and data streams to monitor network-based traffic (including for voice and messaging) to identify potentially fraudulent, illegal, and abusive activity. Among other metrics that factor into the logic for the tool, it can identify a high number of outgoing voice calls with a short duration, including further highlighting abnormal destination dispersion, in any given time period (including shortly

after activation or after a period of relative dormancy if an account or subscription was being “warmed” or aged). It can also detect and flag an origin generating an unusual number or pattern of incoming calls to our network with an atypical origin dispersion in a given timeframe, and identify calls from a number or range of numbers that have been identified as compromised, spoofed, known to be utilized for illegal or other abusive purposes, or otherwise identified as high risk. Once a certain threshold is met, our fraud management system will alert our team, which triggers a fraud investigation. As necessary, our team can and does suspend or terminate the account responsible for originating the abusive activity.

Our commitment to respond fully to traceback requests

We have committed to to fully respond to any and all traceback requests from the Federal Communications Commission, from law enforcement, and from the industry traceback consortium within 24 hours, pursuant to 47 CFR § 64.1200(n)(1) and 47 CFR § 64.6305(a)(2). We also commit to fully cooperating with such entities in investigating and stopping illegal robocallers that attempt to use our network to carry or process illegal calls pursuant to 47 CFR §§ 64.6305(a)(2) and 64.6305(d)(2)(iii).

Certification pursuant to 47 C.F.R. § 64.6305(d)(3)(ii)

Pursuant to 47 C.F.R. § 1.16, I declare, under penalty of perjury, that the statements contained within our foregoing Robocall Mitigation Program description statement and our certification filing are true and accurate to the best of my current information, knowledge, and belief.

On behalf of our customers and team, mahalo nui loa iā ‘oe to you and the Commission for your work on this important program. Should there be any additional information that would be helpful for the Commission in assessing our implementation, please do not hesitate to reach out to me via email to justen@mobi.com or directly at +1 808 500-0555.

Respectfully, ‘o au iho nō me ka mana‘o e kōkua a me ka ‘oia‘i‘o,



justen burdette
chairman + ceo
mobi